THE COURTROOM DEPUTY: Oh, no, the first row. There you go.

THE COURT: Remain standing so you can be sworn in.

J O E L D E C A P U A,

called as a witness having been first duly sworn/affirmed, was examined and testified as follows:

THE COURTROOM DEPUTY: Thank you. Have a seat.

Please state and spell your full name for the record.

THE COURT: You have to try to position the microphone underneath the face shield so you can be heard. You can lift up the microphone stand, if the that makes it better.

THE WITNESS: My name is Joel DeCapua --

THE COURTROOM DEPUTY: Would you make sure the microphone is turned on.

THE WITNESS: Yes. Thank you.

My name is Joel DeCapua, spelling is J-O-E-L, last name, D-E-C-A-P-U-A.

THE COURT: Thank you.

You may inquire, Mr. Moscow.

MR. MOSCOW: Thank you, your Honor.

DIRECT EXAMINATION

BY MR. MOSCOW:

Q Good afternoon, Agent DeCapua.

A Good afternoon.

Q Where do you work?

A I work for the FBI.

Q What's your title there?

A Supervisory Special Agent.

Q How long have you been a Supervisory Special Agent with the FBI?

A I was promoted in 2018.

Q And how long have you been an agent with the FBI?

A I was sworn in in 2009.

Q As an FBI agent, what units or sections have you worked in?

A So originally after I graduated from Quantico, I was assigned to the Newark Field Office where I worked public corruption and white collar crime. In about 2014/2015 I was reassign to the New York Field Office where I worked cybercrime and network intrusions. And I was promoted in 2018 where I went to FBI Headquarters, specifically the cyberdivision, where I worked in the major cybercrimes unit. I was in that unit for approximately 18 months, and then I took a lateral transfer to another unit called the Global Operations and Targeting Unit.

Q And is that where you work now?

A It is.
Q Is the Global Operations and Targeting Unit known by an acronyms?
A We call ourselves GO-TO.
Q So what do you do in GO-TO within the cyberdivision?
A A lot of things. Primarily we provide resources to case teams that are working network intrusions. We provide expert technical expertise. We provide guidance for complicated investigations, and, really, we see ourselves as -- as problem-solvers.
Q All right. You've made a cou8ple of references to "network intrusion." What is a network intrusion?
A It -- it just means when someone breaks into a computer, hackers.
Q So is GO-TO primarily a resource to assist cybercrimes investigators?
A Yes.
Q And is GO-TO typically the lead agency on a case, or are you the unit that's in charge of the case?
A No, we're helpers.
Q All right. What kind of agents do you typically help?
A Cyberagents. People working network intrusions investigations.
Q So when do cybercrimes agent reach out to GO-TO?
A Because we -- we're made up to very experienced agents

who have a lot of experience working cybercrimes, one of my section chiefs called us the "mad scientists."

Q So before you went to GO-TO and while you were there, have you been involved in previously computer-related investigation?

A I have.

Q How many?

A It's hard to put an exact number on it. I would say at least two dozen, upwards of 50.

Q All right. Can you tell us about any particular matters you've worked on?

A Sure. So here in New York, I worked network intrusions that was the result of an insider stealing information from one of the largest investment banks here in New York City. I worked 2014/2015 intrusion of a series of large financial institutions based in United States from someone who is located in Russia and Israel. I worked on an investigation on the network intrusion in the -- the -- of several very large New York-based law firm where someone had entered into their network and stolen all of their email.

THE COURT: Can I get -- I'm sorry, Agent.

Can I have you pull the microphone still closer, because we can barely -- well, I can barely hear you at least?

THE WITNESS: (Complies.)

THE COURT: And maybe raise your face shield or tip your head back a little bit just so you project a little bit better?

Okay.

MR. MOSCOW: Thank you, your Honor.

THE COURT: Go ahead.

BY MR. MOSCOW:

Q So I think in addition to those cases -- well, in connection with those cases, have you received any awards for you cybercrimes investigations?

A I have.

MR. SPILKE: Objection.

THE COURT: Overruled.

Q What awards have you received?

A As an example, I received the Director's Award from an organization FinCen, F-I-N-C-E-N. I received an Exceptional Service Award from the FBI. And I received a Investigator of the Year from the Federal Law Enforcement Foundation.

Q And what is FinCen?

A It is a subagency of the Department of Treasury, and they investigate and regulate money launderers.

Q What did you win an award for from FinCen?

A So it was in relation to a virtual currency exchange that I helped investigate.

Q What about the FBI Exceptional Service Award, what was

that for?
A The Exceptional Service Award was in related to my investigation to the hackers that broke into the law firms.
Q And the Investigator of the Year Award?
A That was in relation to the investigation of the hackers that broke into all the -- the big financial institutions.
Q Can you tell us a little bit about your education background?
A Sure. I bachelor's of Art Degree in economics from DePaul University, and I have a Master's of Science Degree in accounting from Indiana University.
Q Agent DeCapua, do you have any special certifications with respect to cyberinvestigations in the examination of computers?
A I do.
Q Can you tell the jury about some of your certifications related to disk and memory forensics?
A Sure. So related to disk forensics, I have multiple certifications through an agency called GIAC, G-I-A-C, which stands for the Global Information Assurance Credentials.

The first one I can think of is the CFE, which stands for Certified Forensic Examiner. Another one is CFA, Certified Forensic Analyst. And there are others. I would have to have my résumé in front of me.

Q It would help you to remember some of your certifications if we showed you your résumé?
A Yes, absolutely.
MR. MOSCOW: Could we please pull up 3500JBC10, for the witness only?
THE COURT: And I'll remind you, Agent, keep your voice up, even if it's just raising your own volume, as opposed to pulling closer to the microphone, which might be a little difficult.
Q So I think we were discussing some of the certifications related to disk and memory forensics.
A Yes. So disk forensics, Certified Forensic Examiner, which is a course of study and also a four-hour test, I believe, which covers the acquisition of digital media. It covers the analysis of files, the ones that are on disks and the ones that are deleted.
The more-advanced course that I also took and the more advanced certification, the Certified Forensic Analyst, which is continuation of the -- of the CFE certification. And it is more on timeline and user activity, the analysis of logs that are found on a computer system, the analysis of memory. I think those are the -- the two -- do you want me to continue?
Q Those are listed on your résumé as "inactive."
A Yes.

Q What does that mean?
A It means that I didn't pay the fee to reactivate them.
Q And you have a number of certifications. Who typically pays for your recertifications in the fields in which you're certified?
A It's going to be the -- the FBI.
Q So what's "Reverse Engineering Malware"?
Can you describe that certification?
A Yes. So I'm certified in reverse engineering malware. It's basically looking at malware, unwanted computer programs that do something malicious, and determining what it does, where it came from, what its functionalities are, and how to mitigate them on the system.
Q Do you have any certifications related to network forensics?
A I do.
Q What are some of them?
A So there's the Certified Intrusion Analyst Certification, which is looking at low-level networking and how network packets move around the Internet and determining what type of network activity is indicative of malicious activity on the system.
I also have a Network Forensic Analyst Certification, which is just a more-advanced certification. It goes into more depth on digging through packets and

trying to make sense of the 1's and 0's that intercept over a wire.

Q So you've made a number of -- you have a number of certifications relating to forensics. What does that mean?

What are forensics in the context of computers and networking?

A Some call it "digital forensics." It is essentially looking at a computer, looking at the disks, looking at memory, looking at network communications, and just trying to figure out what happened on the computer. What happened over time, and then trying to articulate that for someone else.

Q Do a number of your investigations relate to questions of attribution?

A Yes.

Q What does "attribution" mean in that context?

A Attribution is a term that we use in investigations that basically means who did it.

Q Have you previously been qualified as an expert?

A I have.

Q In what courts?

A The first time was in the Southern District of New York, and the second time was in the Eastern District of New York.

MR. MOSCOW: Your Honor, at this time, I move to

qualify Supervisory Special Agent Joel DeCapua as a expert in the area of networking, malware, and digital forensics.

THE COURT: Do you have any objection, or do you want to go on *voir dire*?

MR. SPILKE: No objection.

THE COURT: All right.

So Agent DeCapua, you are being qualified as an expert in the three areas mentioned by Mr. Moscow. I think it's networking, malware, and digital forensics -- oh, yes, networking/malware was one concept, and then digital forensics -- networking, comma, malware, comma, and digital forensics.

You made proceed.

MR. MOSCOW: Thank you, your Honor.

And, Ms. Laruelle, can you please pull up Government Exhibit 702, which is already in evidence?

And then can we publish it to the jury?

Thank you.

Can we zoom in on the table on the bottom?

Thank you.

BY MR. MOSCOW:

Q All right. Agent DeCapua, what does this table show that we are looking at show?

A It shows logins and logouts on specific times from specific IP addresses.

Q What is an IP address?

A So an IP address, it's acronym. It stands for Internet Protocol Address. And you see four of them right here on the exhibit. They're the four numbers that have the dots in between them.

And at the most basic level it's just -- it's a number that computers use to identify themselves over a network, such as the Internet; and to send and receive packets to other computers connected to the Internet.

Q So how do computers communicate with each other over the Internet?

A So it -- it's very complicated.

On a very high level, communications are made in packets. That's the most atomic form of data that two computers are going to be sending to each other over a network. And every one of those packets is going to have the IP address of the intend recipient of that packet, and it's also going to have the IP address of the source of that packet, who it's from. This is every single network communication over the Internet.

So one -- one good analogy that we kind of like to use when we're trying to explain to people. It's kind of like the U.S. Postal Service, how you have an envelope, and you'll put, you know, the physical mailing address of who you're sending the envelope to and you put your return

address. And it's the same way over -- over a network with packets. Like I said, each packet, it has who it's going to and where it's came from.

Q So is the IP address associated with, for example, where it's going to, is that unique?

A Yes.

Q At what level is it unique? Is it unique to a computer; is it unique to an Internet connection?

A It's unique to -- well, it depends. But in general, it's unique to whatever computer that links that specific IP address. So, for instance, Google.com, the IP address that is hosting Google.com, the famous website, it is going to have its own dedicated IP address. However, my personal Internet access, which I just -- I use an ISP, I'm going to be provided an Internet-access point, a modem, and the IP address is going to be assigned to that specific modem.

Q So before I ask the next question, what is an ISP?

A It's an Internet Service Provider. So it's like Verizon or Optimum or Xfinity.

Q So you have an ISP and a router and a modem here in your home unit, the Internet connection goes through that. Where is the IP address assigned?

A So the IP address is assigned at the ISP. But the IP address is assigned to the equipment that the ISP gave me. So for instance when Verizon assigns me an IP address, it's

assigned to my -- my router and my modem that I have physically at my apartment.

Q If you have a roommate, would your roommate be able to use the same IP address that you were using?

A Yes.

Q At the same time?

A Yes.

Q So if you both check sport scores at the same time and you're Mets fan and your roommate is a Yankee's fan and you both go to the same website, you send information seeking the similar information and with the return address, have the same IP address. How do you know that you will get the right information in response?

A Because one of the jobs of the router is to keep track of which specific device that's connected to it is making which specific requests. So then one person can check the Met's score and one person can check the Yankee score, according to *ESPN*, which is whoever is checking the score, it all looks the same to them, it's coming from the same IP address. Then when it send this return communication with the score, home router determines, Oh, well, this is score that was asked for by Joel's computer; and this is the score that was asked for by the roommate's computer.

Q But as far as *ESPN* is concerned in that example, the IP address just relates to the Internet connection?

A Correct.
Q Okay. And it could mean you or your roommate in that example?
THE COURT: But it suggests you shouldn't be roommate -- we'll leave that for another day.
Q So let's talk about some of the records in this case.
Have you reviewed records obtained from various ISPs in this case?
A I did.
MR. MOSCOW: And we will show what has already been admitted as Government Exhibit 1-A, if we may, Ms. Laruelle?
Thank you.
Q Do you recognize this?
A I do.
Q Does this record show information relating to the video that is in evidence as Government's Exhibit 1?
A It does.
Q What kind of information?
A This shows the upload information. This is provided by Google, which owns YouTube, and it shows the title of the video; it show the time the video was created; and it has the upload IP address.
Q So what does that mean, upload IP address?
A It means that that's the IP address that uploaded the

video to Google, and Google captured that as just part of its normal login process.

Q So that identified the Internet connection from which the video was uploaded to YouTube?

A Precisely.

Q What was the IP address that uploaded this particular video to YouTube?

A 69.125.144.207.

Q For simplicity same, let's agree to refer to that as "the 207 address."

Is that okay?

A Yes.

Q All right. Did you review records in connection with this case showing who used the 207 address?

A I did.

MR. MOSCOW: Ms. Laruelle, could you please pull up what has been admitted as Government Exhibit 554?

Thank you.

Q What is that?

A This is a record that was provided from Optimum ISP.

Q Does this record relate to the same 207 address that uploaded the video?

A It does.

Q Does it show the name and address of user with whom the Internet point is associated?

A The subscriber, yes.
Q What is the name of the subscriber?
A Tawanna Hilliard.
Q And what is the address associated with the Internet connection?
A It's 370 East 31st Street, Apartment 3G, Brooklyn, New York.
Q So what does this record mean?
A It means that the person that was using -- or the person that subscribed the IP address, the 207 IP address on August 6th, 2018, was Tawanna Hilliard Jones.

(Continued on the next page.)

EXAMINATION BY
MR. MOSCOW:
(Continuing.)
Q Ms. Laruelle, can you please publish what has been admitted as Government Exhibit 556.
Do you recognize this document?
A I do.
Q What is it?
A These are additional records that were provided by Optimum.
Q I note that at the top we do not see the 207 address. Is that unusual?
A No.
Q Why not?
A Because IP addresses will change over time. Sometimes you'll have the same IP address from an ISP for a week, sometimes it will be a month. But it's very common for ISPs to reallocate IP addresses over time.
Q And did the IP address in this case change over time?
A It did.
Q Can you turn to Page 5 at the bottom. If we can blow up the very bottom of the page.
So on August 4th and August 5th of 2018, does this show that the same user is assigned to the 207IP address?
A Yes.

Q And can you turn to Page 59 at the top. And if you can make it a little bit bigger and go down a little bit.

And the rest of August 5, 2018 and August 6, 2018, is the same IP address listed?

A Yes.

Q So what does that mean?

A It means that throughout that time period, that IP address, whenever it was used on the internet, it was being used by the device that was subscribed to Tawanna Hilliard.

Q So the Tawanna Hilliard internet connection was assigned that IP address?

A Correct.

Q Could any other internet connection also have been assigned do that IP address?

A No.

Q And taken together with the IP address listed in Government Exhibit 1-A, what does that mean?

A It means that the person that uploaded that YouTube video did so using the internet connection of Tawanna Hilliard Jones.

Q Did you also review records from other ISPs in connection with this case?

A I did.

Q Did you review orders from Oath Holdings?

A I did.

Q Ms. Laruelle, can we please pull up what has been admitted as Government Exhibit 902.

Do you recognize this document?

A I do.

Q What is it?

A This is a record that's provided by Oath Holdings which owns Yahoo showing some subscriber information for the account thilliard31@yahoo.com.

Q Does it list an IP address?

A It does.

Q Is that the same as the 207 address?

A It is not.

Q Is that unusual?

A No, because if you look right below the IP address, you'll see when the account was created when the account was registered and it was in 2003. So, as I mentioned, you would expect IP addresses to change over time especially over this amount of time.

Q Ms. Laruelle, can we please pull up Government Exhibit 903 which is also in evidence.

Can we look for the dates somewhere right around there would be perfect, thank you.

What does this show?

A This shows login activity for that specific user account that I already mentioned, thilliard31@yahoo.com.

Q Is there a login on August 6, 2018?
A There is.
Q What's the IP address associated with that login?
A It's the IP address we've seen before. We've been referring to it as the "207 IP address."
Q And that's the same IP address that uploaded the video titled "NYC Brim Gang Members Snitching. Pt. 1"?
A Yes.
Q Did you review records from any other service providers showing the accounts that used the defendant's IP address ending in 207 at around the time the video was uploaded?
A I did.
Q Ms. Laruelle, could you please pull up Government Exhibit 802 which is also in evidence.

What is this document?

MR. SPILKE: What's the exhibit number, again, I'm sorry.

MR. MOSCOW: 802.

A This is an example of documents that Apple will return in response to a legal request.
Q Can you identify from this document what type of a legal request?
A Yes.
Q What type?
A It's something called a §2703(d) order which is a court

order that, in this specific instance, asks for -- it asks Apple, please let us know who logged in using any Apple service from the 207 IP address on August 5, 2018.

THE COURT: Mr. Moscow, pause for a moment. It occurs to me that one our jurors might have difficulty seeing the witness given the position of the larger TV monitor.

So let me just say to that juror, if you want to, you can also relocate to one of the front seats over here on this side of the courtroom. I leave it up to you, whatever you want to do in that regard. Okay.

MR. MOSCOW: Thank you, your Honor.

THE COURT: You can continue.

MR. MOSCOW: Thank you.

THE COURT: Ladies and gentlemen of the jury, unless someone objects I think we should continue through to 3:30 and not take an afternoon break so we can try to reclaim some of our lost time.

Okay. Go ahead, Mr. Moscow.

MR. MOSCOW: Thank you, your Honor.

EXAMINATION BY

MR. MOSCOW:

(Continuing.)

Q Sir, Apple searched for records showing if anyone logged in it Apple from a 207 -- from the 207 IP address on August 5, 2018?

A That's correct.
Q Did they identify any accounts?
A They did.
Q How many accounts did they identify?
A Just one.
Q What account is that?
A It's the Apple I.D. thilliard31@yahoo.com.
Q Is there a first name associated with that account. And we can scroll to the right on this document. We might go to the first tab.

Have you reviewed all of the tabs of this document?

A I have.
Q And is there one account listed on all of the tabs or one account combined on all of the tabs?
A Yes. Some of the tabs are empty, but the only account that logged in from that IP address at that time was thilliard31@yahoo.com.
Q What is the first name associated with that account?
A Tawanna.
Q Last name?
A Hilliard.
Q What's the address?
A 370 East 31st Street, and I believe there's an apartment associated with it if I just scroll to the right a bit, 3G. I've seen that address I know it's in Brooklyn.

Q Did the Court order any other company to disclose all accounts that logged in from the Defendant's 207 IP address on the date of the video's upload?
A Yes.
Q What other company?
A Google.
Q And did Google find any responsive documents?
A It did.
Q Ms. Laruelle, could you please pull up Government Exhibit 701.
Agent DeCapua, is this one of those responsive documents?
A It is.
Q What's the account name?
A The name is Tyquan Hilliard.
Q What's the e-mail address?
A It's hilliardt90@gmail.com.
Q And it logged into the Defendant's 207 IP address on August 5, 2018?
A Someone from the 207 IP address logged into that account.
Q Did they also logout of that account?
A Yes.
Q Ms. Laruelle, could you please pull up Government Exhibit 702.

Agent DeCapua, is this another one of the accounts identified by Google as having logged in or out from the defendant's IP address the day the video was uploaded?

A Yes.

Q What's the name listed here?

A Prime Time 59 Brim.

Q What's the e-mail address listed?

A It's primetime59brim@gmail.com.

Q Is there a creation date listed?

A There is.

Q What is it?

A It's August 5, 2018, at 1653 UTC.

Q Does it list the IP address from which the user agreed to the terms of service?

A It does.

Q What IP address was used?

A It's the 207 IP address that we identified earlier.

Q On what date?

A It was August 5, 2018.

Q At about what time?

A About 1653 UTC.

Q Ms. Laruelle, could we please pull up Government Exhibit 703.

Agent DeCapua, is this another one of the accounts identified by Google in connection with the request to

determine what accounts logged in to the defendant's internet connection on the date the video was uploaded?
A It is.
Q What's the name on this one?
A It's Tawanna Hilliard.
Q What's the e-mail address?
A It's thilliard31@gmail.com.
Q And if we can go back down to the box below.
Are there a number of login and logout events from the 207 address on August 5, 2018?
A Yes.
Q Were there any logins or logouts on that date from another IP address?
A On August 5th?
Q Yes.
A No, I don't see any.
Q Did Google identify any other accounts that logged in or out from the defendant's IP address on August 5, 2018?
MR. SPILKE: Objection, foundation.
THE COURT: Hold on. Overruled.
A Just those three accounts.
Q So are you able to draw any conclusions from that?
A Yes.
Q What? What do you conclude?
A That the person using the 207 IP address was logging

into the Tawanna Hilliard account, the Tyquan Hilliard account, and the Brims account.

Q So let's talk about the laptop.

Did you examine a laptop and image of a laptop in connection with this case?

A I did.

Q And did you review the contents of a laptop that was marked as Government Exhibit 1000 at the time?

A I did.

Q Was there a computer name associated with the computer that you identified or that you examined?

A There was.

Q Was there also a user name associated with that computer?

A There was.

Q What's the difference between a computer name and a user name?

A Well, on Apple, when you set up an Apple computer, it's going to ask you the very first time you set it up, What do you want your computer name to be? And you can name it whatever you want. And then once that's done, it's going to ask you what user accounts do you want to set up. And then it gives an opportunity to set up a user account. You can use your own name, you can use a nickname, you can use anything you want.

THE COURT: Remember to stay close to the microphone.

Q What was the computer name associated with the laptop in this case?

A It was Tawanna's Mac Book Pro.

Q And how many user accounts were associated with Tawanna's Mac Book Pro?

A It had one user account and one guest account.

Q What was a user account?

A It was duchess_of_bk.

Q Was the duchess_of_bk account password protected?

A It was.

Q Was there a real name associated with the duchess_of_bk user account?

A There was.

Q What is a real name?

A It's called a real name variable. The same time you're setting up your user account on Apple, the first day you get the computer, it's going to ask you what do you want your user account to be. And then it asks you for your real name and you can put your actual name in there if you want to.

Q What was the real name associated with the duchess_of_bk user account in this case?

A It was Tawanna Hilliard.

Q Was there a linked Apple I.D. account associated with

the computer that you examined?
A Yes.
Q What was it?
A It was thilliard31@yahoo.com.
Q So you said that the user account associated with the duchess_of_bk name was password protected. Does that mean if a user wanted to log into the computer but didn't know the password, they could not log in?
A Not to the duchess_of_bk account.
Q Could they log into the guest account?
A Usually, the guest account isn't password protected. I didn't specifically look. I just know that the duchess_of_bk account was.
Q When I examined the computer in this case, did you look for malware on the computer?
A I did.
Q Why?
A Because I had already looked at some of the evidence that we just went through and, as an investigator, I was trying to come up with alternative hypothesis of what could have happened. And the two that came to mind is the common defense that, well, it wasn't me that did the activity it was someone that --
MR. SPILKE: Objection to "common defense."
THE COURT: Hold on one second.

Sustained. So just strike the last sentence and ask another question to elicit whatever information you want from the witness.

Q Did you attempt to determine whether the user of the computer at the time that it was conducting activity on August 5, 2018, was physically in front of the computer or whether it was someone with remote access to the computer?

MR. SPILKE: Objection.

THE COURT: Overruled.

Do you understand that question?

THE WITNESS: Yes.

THE COURT: Okay. Go ahead.

THE WITNESS: Yes. I wanted to determine that the user activity I was observing was actually done by the person sitting in front of the computer and not someone that has remote access to the computer.

Q So did you search for remote access tools like you might find in a network intrusion case?

A I did.

Q What did you find?

A I didn't find any remote access tools. I did find some adware and sometimes they call it potentially unwanted programs.

Q What is adware?

A Adware is it's a type of program that most people

inadvertently download. And it's going to be the type of thing that gives you pop-up windows when you're trying to go on the internet. It's going to -- one common tactic they're trying to get you to pay money to buy a full-service program. It'll say your computer is infected, pay us 20 bucks or install this antivirus. Or it'll say, Your computer needs to be cleaned; get your credit card and pay us 40 bucks in order to get the software that will clean your computer; or it will reroute your traffic. If you just want to go to your home page, instead of taking you to home your page, it'll take you to some obscure search engine, and it'll try to monetize your network traffic by directing your traffic towards places that pay them affiliate fees. It's that type of activity.

Q Can users remotely control a computer using adware like you found on the defendant's computer?

A No.

Q Was there anything in your examination that was suggestive of somebody else having control over the computer?

A I found no evidence of that.

Q Did you also look for an updated operating system?

A I did.

Q Why did you look for that?

A Because one of the biggest indicators of whether a system is vulnerable to someone gaining remote access is going to be if the computer has all the most current updated

security patches. And I knew that if on August 5, 2018, it was a fully updated operating system with all the security patches installed, that it was less likely that someone was going to be able to run some type of malware on the computer that gave him remote access.

Q Did the computer that you examined have an updated operating system?

A It did.

Q So, based on your analysis, was anyone other than a person with access to the password protected duchess_of_bk user account on the computer using the defendant's computer on August 5, 2018?

A No.

Q And before we get any further, let me show you Government Exhibit 1000.

MR. MOSCOW: Your Honor, may I have permission to approach?

THE COURT: Yes.

(Approaching the witness.)

Q Is that the computer that you examined in this case?

A Yes.

Q Did you analyze the activity of the user of that computer on August 5, 2018?

A I did.

Q And when we say, "Activity," what do we mean? What did

you analyze?
A I just wanted to know around the same time that the YouTube video was uploaded what was going on on this specific computer.
Q So what did you look at when you looked at the user activity?
A Well, I note -- I looked at logs, log files. Whenever a user uses -- does anything on a computer, it's creating a trail of logs that lets someone like me be able to analyze the logs and figure out what happened over time. And I know that when someone wants to upload something to a site like YouTube, they're going to have to use a web browser. So one thing in particular I was looking for was some type of internet history.
Q You mentioned log files. Approximately how many log files did you identify on the computer?
A A lot. I can't give an approximate number.
Q Are the log files easily understood to a layperson?
A It depends on the log file. In general, no, you have to specifically know what you're looking for and you have to have the tools to enable to allow you to extract useful information from them.
Q And were you able to prepare a summary showing a small volume of information that you were able to parse from the many log files that you examined?

A I did.
Q Did that file include URLs and other things that are easily understood in the format that they are presented?
A Yes, in the format that I presented them.
Q But not in the format they existed natively?
A No.
Q Is there also a screenshot of at least one page to which you navigated during your investigation containing your summary exhibit?
A Yes, a website.
Q Ms. Laruelle, can we please show the witness only Government Exhibit 1311.

Do you recognize this?

A Yes, I made it.
Q Is this the summary chart that we were just talking about?
A It is.

MR. MOSCOW: Your Honor, the Government asks permission to move Government Exhibit 1311 into evidence.

THE COURT: Any objection?

MR. SPILKE: One moment, your Honor.

THE COURT: Government Exhibit 1311 is admitted.

MR. SPILKE: I said one moment, your Honor.

THE COURT: I'm so sorry.

MR. SPILKE: May I voir dire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MR. SPILKE:

Q Government's Exhibit 1311, did you create this?

A I did.

Q How did you create this?

A Well, I parsed a log file that I knew was going to have web history in it. And I took that log file and I changed the encoding of it in order to present it so someone, just a layperson, could read it and understand that it's a URL that references a specific website.

Q And how did you change the encoding?

A So there's a couple steps. First, I pulled the actual URL out of "A" File called FS Events which is a log file that just keeps track of changes to the file system, to an Apple OS file system.

And I knew the specific ones that I pulled out of this log file were relevant to me because I know that in 2018 when this computer was imaged it was running Mac OS Sierra, that was the name of the operating system. And Safari on that operating system saves history files to a location called History. And the way it saves those files, if I went to the site Google.com, it's going to write "A" File in that history folder that's going to say http://google.com. And then if I go to Yahoo.com, it's going to write another file

in that same folder.

When I looked on this computer that folder was empty there was no history. So in order to reconstruct what used to be in that history file, I went to the log file I mentioned FS Events, which, as I mentioned before, keeps track of changes to the file system.

So any time anything is written on the file system, or anything is deleted from the file system, there is going to be a log entry in FS Events.

So I used a tool made for analyzing FS Events and then I found the specific FS Event files where the activity relevant to August 5, 2018, was. And then knowing where those specific files were, then I used a text editor to, well, first I had to decompress the file they were stored in "A" File compression format called Gzip. So I decompressed compressed the file and then I had, we call it plain text. So I saw a plain text which is human readable, the human readable URL but it was ill encoded in something called URL encoding or percent encoding which means --

THE COURT: What was the second word? Percent?

THE WITNESS: Percent encoding.

THE COURT: Percent encoding.

THE WITNESS: Percent encoding.

A And what that is where the slashes in a URL, instead of being a slash, to will just say percent, and then will be two

bytes, I think it's FE or a forward slash but I'm a hundred percent sure about that.

And so, from the percent encoded URL, then I just decoded from percent encoding into plain text and then populated this spreadsheet which I created showing the history for that specific time period.

Q And how did you convert the percent encoding to the format we're looking at now?

A So because --

Q Did you do it by hand or did you have a script that does it, something like that?

A So I did it by hand which is kind of embarrassing. But there wasn't enough -- it didn't make sense to build a script or to use a tool because there wasn't enough of it. So I just went through and I looked for all the percent FEs and deleted them and put a slash.

Q And I see that there's a timeframe here. It says 4:10:30 UTC or approximately 5:34 UTC.

A Yes.

Q Does this exhibit represent all the events that took place on that laptop between those times for that user --

A No.

Q -- duchess_of_bk? Sorry.

A No, it does not.

Q No, it does not?

A No.
Q Do you know approximately how many were omitted?
A So how many web history of FS Events, or how many just the FS Events in general?
Q How many web history FS Events?
A So not many. There were some, there was some. But they -- it was like browsing. It wasn't related to this case. It wasn't -- I just picked the stuff that was Google and YouTube.
Q And you're the one who chose which FS Events, or rather, which URLs to show here?
A Yes.
MR. SPILKE: Okay. Nothing further. No objection.
THE COURT: All right. Can you clarify one thing.
When you say these are selective ones, it's still within a timeframe, though, right? So they're restricted by timeframe? In other words, could there be other FS Events outside of this time range or not on this date that you didn't include?
THE WITNESS: Certainly. With respect to browsing history, there's about a month of browsing history. And, again, I just looked at the one day.
THE COURT: Okay. Go ahead, Mr. Moscow. 1311 is admitted.
(Government's Exhibit 1311 was received in evidence

as of this date.)

MR. MOSCOW: Thank you, your Honor.

DIRECT EXAMINATION

BY MR. MOSCOW:

(Continuing.)

Q So again, you saw that there was nothing in the traditional place where a computer would store internet history; is that right?

A Correct.

Q But that didn't mean that the user never navigated to a web page?

A Correct.

Q It meant that the history simply wasn't there?

A That's correct.

Q So then you described going to the FS Events log file. You've identified, and I think we have put on the chart, a number of URLs.

MR. MOSCOW: And if we could have permission, your Honor, at this time to publish Government Exhibit 1311 to the jury.

THE COURT: Yes, of course.

(The above-referred to exhibit was published to the jury.)

Q You previously mentioned that the URLs below here on Page 1 are URLs associated with a specific timeframe?

A Yes.
Q What does that mean?
A It means that I know -- I don't know the exact date that the user browsed to these specific URLs, I just know that the activity what happened on August 5, 2018, between 4:10 p.m. and 5:34 p.m. UTC.
Q How do you know that?
A So I know that because of the way that FS Events works is when a user is using their computer in the background there's a service called FS Events. And it is just constantly keeping track of any changes to the file system and it's storing that information into memory.

Now, periodically, the amount of memory that it allocated for these types of log files it gets flush the out of memory and written on to the disc.

Now, I don't have access to the memory on August 5, 2018, I just had access to the disc from when the computer was actually seized. So I can go into the hidden location where FS Events log files are stored and I can see all those separate files where the memory was flushed and written to disc. And all those separate files have date stamps, creation date stamps, associated with them.

So for this specific exhibit we're looking at, the URLs that I found were in one of those specific files and the creation date of that file was on 5:34:04 of 8/5/2018. So I

know this activity doesn't include anything after that date. And that I also know because this wasn't the first log file in there, there was other log files previous to it, that this activity only begins on the creation date of the last log file. And the creation date for that was August 5, 2018, 4:10 UTC.

So that's how I can logically assert that the URLs I found in this specific log file must have been created between those two time -- in that timeframe between the creation date of those two files.

Q So, based on your review of the log files that were saved, or the creation date of August 5, 2018 at 5:34 p.m. UTC, was there any internet activity associated with the guest account?

A No.

Q Was there any internet activity associated with the duchess_of_bk account?

A Yes.

Q What kind of activity?

A So somebody was creating a Google account, and you see that in the bottom two entries of this exhibit where it says accounts.google.com web create account, that's the first page you click when you sign up for a new account. And when you start going through the process and entering what your Gmail account would be and then it takes you to a second page which

is web personal details, and that's where you put in your name and date of birth and information like that, telephone number, if you want to. And then, on the second page, there's more.

Q Is the second page from the same time period, just more URLs?

A Yes, it just didn't fit on the first page. And so, here you see at the very top the completion of the creation of that Gmail account. It's web terms of service where it says do you agree to the terms of service and you have to click the little box and this is the URL that Google is going to send you to to finish your account signup.

Q Is there anything associated with a YouTube page in this timeframe?

A There is.

Q Can you blow up some of the -- thank you.

Now, what do you see there?

A So I mean, the plain text of the URL shows YouTube.com/create_channel. And then below you see the YouTube.com/upload.

Q Is there a page YouTube.com/verify_phone_number?

A Yes.

Q Are they had listed in temporal order?

A No.

Q If we can scroll up a little bit. Are there any pages

associated with Google Drive?
A Yes.
Q What is, for example, drive.google.com/drive?
A That's a -- if you are signed up to Google Drive, you can store files. And this is if you log into your Google account and you try to navigate to where your stored files are, this is one of the URLs that you are going to come to as you navigate to find the file you want.
Q So after this -- the file containing these URLs containing evidence that the duchess_of_bk account navigated to these website was written to the hard drive at about 5:34 p.m. UTC, was there another log file opened?
A There was.
Q And can you go to Page 3. Does that show more internet activity of the duchess_of_bk user on August 5, 2018?
A It does. This log file had a lot less, or a lot fewer, URLs.
Q So what was in this log file?
A I was able to identify four web history files. That's from Google.
Q What is the support Google page that's contained here?
A So I went to that page. It is a help page from Google that gives advice on uploading YouTube videos longer than 15 minutes.
Q Did you document that page in any way?

A I did. I took a screenshot.
Q Can we go to Page 4.
So based on the files that we have seen so far, what conclusions were you able to draw?
A I was able to -- someone was logged into the duchess_of_bk account and was browsing the internet on 8/5/2018 and they created a Google account. And then they use -- then they went to YouTube and created a YouTube account. And then they went to URLs that said YouTube_upload. And then, shortly thereafter, looks like they navigated to a support page that is giving advice on uploading videos longer than 15 minutes.
Q Was there any more internet activity after the stuff that you observed referenced in Page 3?
A Yes.
Q Can you go to Page 5.
THE COURT: Of Exhibit 1311?
MR. MOSCOW: Still in Exhibit 1311, your Honor.
Q What does this show?
A This shows more web browsing activity.
Q So in the period -- is this the next log file after the log file that we just discussed?
A Yes.
Q So in the log file, after the user of the duchess_of_bk account went to a help page for uploading YouTube videos

longer than 15 minutes, what did they do? What did the user do?

A So, based on the URL that's here, it looks like they navigated to Google and then changed their account to be logged the in from the thilliard31@gmail account based on the very top URL.

Q And then did anyone view a YouTube video?

A Yes, down at the bottom you can see the YouTube activity.

Q Did you review any other activity of the user other than internet activity?

A I did.

Q Let's talk about some of that.

Did you review any Apple Notes in connection with your review of the computer?

A I did.

Q What is an Apple Note?

A If you use Apple services, whether it's an iPhone or whether it's their computers, it gives you an opportunity to leave notes for self. These are like the "buy a gallon of milk," or "take out the garbage," or "remember to call this person." And the note that you leave yourself in your iPhone is going to be synced across all your devices to include your laptop or your iPad or whatever else you have in the Apple ecosystem.

Q Did you review all Apple Notes in connection with this case?
A No.
Q How did you view the Apple Notes that you did view?
A So Apple Notes are stored on a Mac computer in a very specific place. And it's stored in something called a SQLite database. And when I was analyzing this computer I found the SQLite database for -- that stored the notes activity and I opened it up and looked at the specific relevant date here, August 5, 2018, to see if there were any notes.
Q And did you document that process?
A I did.
Q Can we go to Page 6 still of Government Exhibit 1311.

What does this show?

A This is a screenshot I took of a tool I used for querying a SQLite database called DB Browser for SQLite. In particular, this show me running a query in order to pull the two notes that I found that were relevant around the relevant time period that had to do with the YouTube video in question.

THE COURT: Mr. Moscow, you have a couple more minutes before we break for the day and for the week.

MR. MOSCOW: Thank you, your Honor.

Q Did you review an Apple Note that was created at, approximately, 4:50 p.m. UTC time?

A I did.
Q What was in the note that you reviewed?
A Well, there was a column called Z Snippet which said first: Primetime. In the column called, Z Title 1, it said primetime59brim@gmail.com/primetime59.
Q And was there any other information associated with that note that's not captured here?
A There is. So on a separate table, there is another column called Z Data where Apple Notes will write -- if something, if the note is too long to fit in the Z Snippet area, then it will write it to the Z Data column. And in the Z Data column, after decoding it, I found there was a -- it said first Primetime and then it said last, 59Brim. That's not here but I found that, also.
Q In the course of your investigation of this image of the laptop, did you review other notes saved by the duchess_of_bk user?
A Very cursory, but yes.
Q Did you view a pattern of storing information in Apple Notes?
A Yes. So it looks like she would store passwords, user accounts, and passwords sometimes using Apple Notes.
Q Based on your review of the Apple Notes that you saw, do you have an understanding of what the Z Title as to note 786 meant?

A I don't know for sure but it uses the same pattern that she would store, you know, user accounts and passwords.
Q And did you also review an Apple Note that was created approximately six minutes later?
A I did.
Q In those six minutes -- sorry, is that note 787 reflected on this chart?
A Yes.
Q What is the Z Title associated with that?
A It is NYC Brim Gang Member Snitching. Pt. 1.
Q So in the six minutes between the saving of the first Apple Note and the saving of the second Apple Note, did anything of significance happen with respect to this investigation?
A I don't recall specifically. I would have to see my notes.
THE COURT: So why don't we break here since we're right at 3:30 and the witness will then continue on Monday. And then you can have, in the interim, look at your notes or perhaps we should do that on the record. I take that back.
Sir, you can step down and you're excused.
Maybe have a seat let me excuse the jury first, my apologies. Let me do that because I want to get them on their way.
Ladies and gentlemen, that concludes today and this

(Jury enters the courtroom.)

THE COURT: Good morning ladies and gentlemen. It's nice to see you all here today. I hope you had a wonderful weekend and maybe enjoyed the nice weather we had. We're going to resume now with the testimony of Agent DeCapua. Agent, I remind you that you're still under oath.

DIRECT EXAMINATION

BY MR. MOSCOW:

Q Good morning, Agent DeCapua.

A Good morning.

Q When we left off, I think you were walking us through two Apple notes you found on the defendant's user account on the defendant's computer.

MR. MOSCOW: Ms. Laruelle, can you please publish Government Exhibit 1311 at page 6?

Q Would it be possible to remind the jury what the first Apple note that you found note 786 said?

A It said first Primetime, last brim. Primetime59brim@gmail.com/primetime59.

Q When was that note saved?

A On August 5, 2018, at approximately 16:50 UTC.

MR. MOSCOW: Ms. Laruelle, can we publish what's been admitted as Government Exhibit 702?

Q You testified on Friday about this document too, right?

A Yes.

Q What does this show again?

A This is a document provided by Google showing the account information for the e-mail address Primetime59brim@Gmail.com.

MR, MOSCOW: Can we just highlight the line where it says, created on, and blow it up?

Q So when was the Primetime59brim account created?

A August 5, 2017, at 16:53 UTC.

Q About how long after the note was saved on the defendant's user account on the defendant's computer was the Primetime59brim account created?

A A few minutes.

Q And if we can please return to Government Exhibit 1311 at page 6.

The other note that you talked about was note 787. What does note 787 say?

A It says NYC Brim gang members snitching, part one.

Q What time was that note saved?

A August 5, 2018, at 16:56 UTC.

Q About how long after the Primetime59brim account was that note saved?

A A couple minutes.

MR. MOSCOW: Thank you very much. No further questions.

THE COURT: Thank you very much, Mr. Moscow.

You're witness, Mr. Spilke.

MR. SPILKE: May I inquire, Judge.

THE COURT: Yes. Of course.

CROSS EXAMINATION

BY MR. SPILKE:

Q Now, you testified a little bit about a type of file calls FS event logs, yes?

A Yes.

Q And an FS events log is basically what now?

A It's a log that Mac OS keeps that records changes to the Apple file system over time.

Q And changes made by a user?

A So it be a user or it can be the operating system.

Q So it's both. The user or operating system. FS events would, sort of, record that?

A Yes.

Q And things get deleted from FS Event logs sometimes, right?

A They do.

Q They get overwritten?

A I wouldn't say overwritten, but they will get purged.

Q Purged? Meaning no longer on the system at all?

A Yes.

Q And now, I don't know if you've gone into this, but what tools did you use to search the FS Event logs?

A So there's several forensic tools that are built for taking FS Event event logs and taking it from the binary format that the operating system saves it and making it so someone like me can easily reference it in, say, an Excel spreadsheet. So there's a couple automated tools that I ran that did this automatically. One was, I believe FS Event parser, and the other one was Mac APT. Now, those are the automated tools that I used. I also went in manually and just confirmed the information in the automated tools by decompressing it myself and looking at the actual log files myself.

Q And the first thing you mentioned was FS Event what now?

A FS Event parser.

Q Parser.

And can you do keyword searches in that.

A The output that the program gives you is something called a tab separated value, which is something you can open up in Excel and you can do keyword searches in Excel.

Q And then the Mac APT, can you do keyword searches in that?

A The output of Mac APT is an Excel document. So it's as easy as doing a keyword search within Excel.

Q Are you aware of a program called Axiom, A-X-I-O-M?

A I've heard of it. I have not used it.

Q You're aware, of course, that you can do keyword searches of FS event logs from Axiom, right?

A I don't know that.

Q Have you ever heard of FTK?

A I have.

Q What's that?

A It's a forensic tool that is highly popular with particularly data carving and file carving.

Q And you can do keyword searches from FTK, right?

A Correct.

Q Keyword searches -- just to be clear. Keyword searches of the FS Events logs, right?

A So I don't know that for sure because FS Event is -- it's compressed in a particular way. So I don't know if FTK or Axiom actually has some type of -- something that will decompress it and decode it and make it available to the analyst.

THE COURT: I'm going to pause you for one second. Just for the court reporter. I think the word you used is data carving, correct?

THE WITNESS. Yes.

Q And forensic explorer, is that a tool that you you've used?

A It sounds familiar. I don't know if I've used it before.

Q Are you aware that's also a tool that you can use to search FS Event logs?

A I don't know that.

Q And then encase, E-N-C-A-S-E. Do you know what that is?

A Yes. Another forensic tool.

Q And is that another tool that you can use to run keyword searches on FS Event logs?

A Again, I don't know if -- I don't know if it will parse the FS Event logs.

Q But at least the tools that you used; FS Event parser and Mac APT, they spit out an Excel document, right?

A Yes.

Q And from that Excel document you can do a keyword search, right?

A Yes.

Q And just to be clear, the only references that you found to Primetime59brim were on August 5, 2018, right?

A The only place I was looking was around August 5, 2018.

Q You didn't look on any other date?

A So in particular with the FS Event logs, the first filter I used was just looking for web history. And so within that web history, there's like a month of stuff. And so I did scroll down and I looked at the entire month of the web browsing history. But the only thing I was really

zooming in on was what happened right around the time that the YouTube video was uploaded.

Q Right. But you weren't prevented from looking at other dates, right?

A No.

Q Just to be clear. The only references you found --

MR. SPILKE: Can we pull up actually Government Exhibit 1311, which is in evidence.

Q Let me just show you pages 1 and 2 of that. These were the only references to primetime59brim --

MR. SPILKE: Withdrawn.

Q All the references you found to primetime59brim, you put into Government exhibit 1311, right? You can keep scrolling if you need to. Do you need to look at the other pages?

A No, I'm trying to think.

Q Well, if you had --

MR. SPILKE: Well, I'll ask a different question.

Q If you found other references to Primetime59brim on that laptop, you would have put it into Government Exhibit 1311, wouldn't you have?

A By the time I was creating this particular demonstrative, I was already completely zoomed in on just the notes and on the web browsing history. But I'm trying to think more broadly if I found any other references. I'm

not sure.

Q So if you had found other references to primetime59brim, you would have left it off this exhibit?

A Well, sometimes there's other references within a file system but it's just echoing something that has already been said. So like, for instance, I wouldn't be surprised if you would search the file system and find another reference. Yet it's some type of metadata or some type of log reflecting activity that has already being laid out in the exhibit I made.

Q So meaning it would basically be duplicative. You wouldn't put a duplicative entry in there?

A Correct.

Q But those are the only ones you would exclude, right? Duplicative entries?

A Duplicative entries are I think are just entries I can't explain. Like, for instance, FS Event I understand what that is. I understand what it means when something shows up in FS Event and I can come up here and explain it to you.

Q Now, this FS Event log, it records the file system activity?

A Yes.

Q And there are thousands, perhaps hundreds of thousands of FS Event created, let's say, in a month, right?

A Yes.

Q And modern file systems write these FS Event logs sometimes by the millisecond, right?

A Yes.

Q So you can have hundreds in one second?

A Yes.

Q And are you aware of how many FS Event were on that laptop total? Thousands?

THE COURT: For what period of time? Or you mean everything?

MR. SPILKE: Everything that he had access to.

A Off the top of my head -- remember, FS Event writes things into separate log files within a folder and I want to say there was between 50 or 60 of those separate files. But then when looking inside of each of those files and pulling out the actual log entries, it was over a million entries.

Q Okay, okay. And it's in what's called a dot folder, right? D-O-T?

A Yes.

Q Do you know what that is?

A It's -- it means it's a hidden file. It's a hidden folder on the Mac OS system.

Q Meaning -- I don't have it in front of me, but I think the folder itself was like slash dot FS Event? Something like that, right?

A Yes.

Q And that's to, sort of, hide it from the average user, right?

A Yes.

Q It's sort of a signal. Average user don't go in here, right?

A It's more of a signal of that finder, which is what an average user would use to browse the file system, finder just wouldn't even show it to the user.

Q Because if a user without any training went in and started maybe moving certain files it would sort of mess up the function of the computer, right?

A I don't know about that.

Q And if you if you started deleting files from the FS Event folder, it could compromise the functioning of the computer, right?

A So, I don't know.

Q Do you know what log-in credentials are?

A Yes.

Q Now, you're aware, aren't you, that logging in to, let's say, an e-mail account or a Google account, that would be recorded in FS Event, right?

A I can't think of any reason that logging into a Google account would result in a change to the Apple file system.

Q Now let me ask you this. Sometimes when you go to your

-- to any password protected account, sometimes the user name is auto populated, right?

A Yes.

Q But sometimes the user enters it, right?

A Yes.

Q Same for the password. Sometimes it's auto completed, right?

A Yes.

Q And sometimes the user enters it, right?

A Yes.

Q You weren't able to tell whether the user entered log in credentials during the time that you looked at the FS Event logs, right?

A For which specific account?

Q So can we pull up -- you testified about three accounts I believe. And that was Government Exhibit 701, 702, 703. Do you remember those series of questions?

A I do.

Q I think there was a THilliard31 account?

A Yes.

Q There was a Primetime59brim account?

A Yes.

Q And there was another one that had to do with Hilliard. I think it was for --

A Hilliard T.

Q Hilliard T, something like that, right?

A Yes.

Q Now, I think you testified there was some logging on and logging off activity?

A Correct.

Q All that was on August 5, 2018?

A According to Google, correct.

Q But with -- you had the hard drive. You couldn't -- you didn't -- you weren't able to determine whether the username was put in by a user or whether it was auto-completed, right? You did not make that determination?

A That's not something I even looked at.

Q For all three accounts. Same answer, right?

A Correct.

Q Let me ask you something about -- you said there were two, I think profiles or accounts. There's the guest and the Dutchess of BK. What are those; profiles or accounts?

A You can use it almost interchangeably.

Q Now, are those partitioned? Am I using that word correctly?

A I don't think so. I don't think you're using the word correctly.

Q What kind of access would the guest account have to the Dutchess of BK account, for instance?

A So on a typical Mac OS account, the guest account won't

have access to any of the files or log files recorded under the Dutchess of BK account.

Q Sometimes it won't even have access to like the apps right?

So let me just ask you this.

If the Dutchess of BK, that account, has Microsoft Word, the guest wouldn't necessarily have access to that Apple, right?

A Not necessarily.

Q And same goes for like iTunes, right?

A Correct. But it depends on how it's configured and how Dutchess of BK would give access to apps to the guest.

Q Right. But that would have to -- it's not by default that the guest has access to everything that's under the password protected account?

A I don't know for sure.

Q So files saved on the Dutchess of BK account wouldn't necessarily be accessible by the guest account, right?

A That's correct.

Q And I think you testified yesterday that whoever was using the Dutchess of BK profile did all of that activity that you put into Government Exhibit 1311, right?

A Yes.

Q You don't know who was using that profile, right?

A It was the person who logged into the account.

Q Well, the person that logged into the account would have passed the computer over to someone else, right?

A If they had their password, yeah.

Q Well, every time you pass a computer to someone, you have to put in the password?

A If it was already unlocked and they passed the computer, then yes.

MR. SPILKE: Okay. One moment, please. No further questions.

THE COURT: Thank you, Mr. Spilke. Any redirect?

MR. MOSCOW: No, your Honor.

THE COURT: Thank you very much, agent. You may step down and you're excused.

Does the Government have any more witnesses or evidence to present?

MR. MOSCOW: Your Honor, at this time, the Government moves Government Exhibit 952 into evidence. And we would ask to publish it briefly to the jury.

MR. SPILKE: No objection.

THE COURT: 952 is admitted and you may publish.

(Government's Exhibit 952 received in evidence.)

(Continued on the next page.)